EMAIL POLICY MANAGER

This invention relates to an email policy manager, for use
in an email system. More particularly, the invention may
5   be applied to a boundary agent, and a method used therein,
for applying email policy.

Email is a convenient way for computer users to
communicate, and in particular provides a very convenient
10   way for a computer user to transmit data to another
computer user.

However, this very convenience means that it is important
for an organization to be able to carry out at least some
15   forms of monitoring of emails sent from the organization.
For example, emails may be used to send confidential
information to unauthorized recipients outside the
organization. As another example, emails may be used to
send attachments in the form of program executables. This
20   can lead to another difficulty arising from the use of
email, namely the spread of computer viruses, which may be
sent as executable file attachments to emails.

Many of these problems are solved to a large extent by the
25   use of email manager software, that is, a software
application which is provided on a local area network
(LAN), and monitors emails. In particular, a boundary
agent is a software application, which is provided on a
local area network (LAN) having an internet connection, and
30   monitors emails being sent over the internet by users
connected to the LAN.

The boundary agent can then detect emails whose attachments
may contain viruses. Similarly, the boundary agent can
35   detect emails whose content is suspicious. For example,
emails containing specific key words can be regarded as

suspicious. Also, emails having large attachments, or specific filetypes as attachments, can be regarded as suspicious.

5   Suspicious emails can be blocked, or they can be quarantined, that is, they are not transmitted at least until they have been reviewed. The rules, which are set up by the organization to determine which emails are treated as suspicious, are termed an "email policy".

10

Examples of boundary agents are products in the MIMESweeper® range from Clearswift Corporation.

One feature of boundary agents is that they can allow the
15   email policy to be user-dependent. In particular, considering the application of the boundary agent to monitoring outgoing emails, the rules, which determine which emails are treated as suspicious, can vary from one user to another.

20

For example, while some personnel within an organization may be expected to send emails dealing with a particular subject, other personnel may not be expected to send emails dealing with that subject. In that case, emails containing
25   key words relating to that subject may be treated as suspicious if they are sent by personnel within the second group.

Similarly, while some personnel within an organization may
30   be expected to send emails with attachments of specific types, such as spreadsheets or image files, other personnel may not be expected to send emails having such attachments. In that case, emails having that type of attachment may be treated as suspicious if they are sent by personnel within
35   the second group.

WO03/001326 discloses an email policy engine, which
receives a message, and then determines from the sender
which policy to apply to that message. Depending on the
identity of the sender, the policy may determine whether or
5   not a digital signature on the email should be verified.

Boundary agents applying such user-dependent email policies
use the "From" field in the email message to identify the
sender of the message, and then determine the rules which
10   are to be followed for that user's messages.

However, this has the disadvantage that the content of the
"From" field is no guarantee of the identity of the sender
of the message. For example, a desktop email creating
15   program may allow a user to create multiple accounts, and
to complete the "From" field at will when creating such
accounts. In this way, it becomes possible that, if a user
knows the content of the "From" field in messages sent by
another user, he can enter the same content in the "From"
20   field of his own outgoing messages. The user is then
subject not to the intended email policy, but to the email
policy which applies to the other user.

WO01/37496 discloses an alternative email policy manager.
25   In this system, depending on the identity of the sender,
the policy may determine whether or not to add a digital
signature to the email and whether or not to encrypt the
message. Again, the system uses the "From" field in the
email message to identify the sender of the message, and
30   then determines the policy to be applied on that basis.
However, again as mentioned above, the content of the
"From" field can be forged, and is no guarantee of the
identity of the sender of the message.

35   It is known in other circumstances that digital signatures
can be used to identify the sender of email messages. For

example, US-5,956,408 describes a method for distributing
data, in which data is encrypted using a private key of the
data sender, and digitally signed by the sender. The
recipient decrypts the encrypted data, using a public key
5   of the data sender, and verifies the digital signature. If
the digital signature is verified, the decrypted data is
enabled for use.

However, as in the example given above, digital signatures
10   are typically used only by a recipient of a message to
confirm the identity of the sender or the validity of the
message, after the message has been transmitted across a
network.

15   Somewhat similarly, US Patent Application No. 2003/0135737
discloses a system for use by a service provider, in which
the service provider determines whether to forward a
received message, based on verifying the signature in the
message.
20
By contrast, according to an aspect of the present
invention, there is provided a method of applying an email
policy to determine whether a message should be allowed to
be transmitted from a local area network across a wide area
25   network. The method according to the present invention
applies a sender-dependent policy, using a digital
signature to identify the sender of a message.

This has the advantage that the digital signature allows
30   the sender to be identified with a high degree of
certainty, so that the sender-dependent policy can be
applied correctly.

According to another aspect of the present invention, there
35   is provided a computer program product containing code for
performing the method.

For a better understanding of the present invention, and to
show how it may be put into effect, reference will now be
made, by way of example, to the accompanying drawings.

5

Figure 1 is a block schematic diagram of a computer
network.

Figure 2 is a flow chart, illustrating a method according
10   to the present invention.

Figure 1 shows a computer network 10, which includes a
local area network (LAN) 15, having personal computers
(PCs) 16, 17, 18, 19 connected to it.   The LAN has a
15   connection to a wide area network (WAN) 25, which in this
illustrated embodiment is the internet.   Also shown
connected to the internet 25 is a further personal computer
(PC) 30.   It will be appreciated that a real computer
network is very much more complex than that illustrated,
20   but the network shown in Figure 1 is sufficient to
illustrate and explain the present invention.

One common use of a computer network, such as that shown in
Figure 1, is to transmit electronic mail messages.   For
25   example, the user of one of the personal computers 16-19
can transmit electronic mail messages to the user of the
personal computer 30.   Such messages can contain text
alone, or they can have attachments in the form of computer
files.

30

As shown in the Figure 1, the local area network 15
includes a boundary agent 32, which takes the form of
software running on a mail server (not shown) in the
network 15.   The boundary agent 32 inspects the email
35   traffic, which is intended to be transmitted over the

internet 15. For example, the boundary agent 32
automatically checks mail messages for viruses.

In addition, the boundary agent 32 applies a sender-
5   dependent email policy. Thus, while some personnel within
an organization, that is, some users of personal computers
16-19, are permitted to send emails with attachments of
specific types, such as spreadsheets or image files, other
personnel are not permitted to send emails having such
10   attachments. The boundary agent 32 can be generally
conventional, and will therefore not be described further
herein, except as required for an understanding of the
present invention.

15   Figure 2 is a flow chart, showing a method performed by the
boundary agent in accordance with the present invention.

In step 70, the boundary agent 32 inspects a mail message,
which has been transmitted from one of the personal
20   computers 16-19, intended for an external computer user,
for example a user of the computer 30.

In step 72, the boundary agent 32 determines whether the
message contains a digital signature and, if so, the
25   boundary agent 32 determines in step 74 whether the digital
signature can be verified.

A digital signature is a code which can be incorporated in
an electronic mail message in order to identify the sender
30   of the message. Conventional desktop email creating
programs incorporate a feature allowing a digital signature
to be added. As is known in the art, an infrastructure
must be provided to allow the verification of digital
signatures, and this will not be described in detail
35   herein. Briefly, it is possible to verify a digital
signature by checking with a Certification Authority, which

maintains (either directly or indirectly) a list of valid
digital signatures and the identities of the associated
users.

5   If it is determined in step 72 that the message contains a
digital signature, and if the digital signature is verified
in step 74, the process passes to step 76. It should be
noted that the verification of the digital signature may
also confirm that the message has not been compromised
10   during transport.

In step 76, the process applies a sender-specific email
policy. That is, having extracted the purported identity
of the user from the message, and having verified that the
15   digital signature applies to the same user, the boundary
agent 32 determines whether the message, and any
attachments, comply with an email policy which is specific
to the user identified in the message. For this purpose,
the boundary agent 32 maintains a list of users, and the
20   respective email policies which are to be applied to
messages sent by those users.

For example, while some users of the personal computers 16-
19 may be expected to send emails dealing with a particular
25   subject, other users may not be expected to send emails
dealing with that subject. In that case, emails containing
key words relating to that subject do not comply with the
sender-specific email policy, if they are sent by personnel
within the second group.
30
Similarly, while some users of the personal computers 16-19
may be expected to send emails with attachments of specific
types, such as spreadsheets or image files, other users may
not be expected to send emails having such attachments. In
35   that case, emails having that type of attachment do not

8

comply with the sender-specific email policy, if they are
sent by users within the second group.

If it is determined in step 76 that the message complies
5   with the sender-specific email policy, the process passes
to step 78, and the message is allowed to be transmitted
over the internet 25. By contrast, if it is determined in
step 76 that the message does not comply with the sender-
specific email policy, the process passes to step 80, and
10 appropriate measures are applied.

For example, the message may be blocked, with or without
notification to the sender, or may be quarantined for
review by IT personnel responsible for operation of the
15 local area network 15, or, in the case where it is an
attachment which causes non-compliance with the email
policy, the message may be transmitted without the
attachment.

20 If it is determined in step 72 that the message does not
contain a digital signature, or if is determined in step 74
that the digital signature is not verified, the process
passes to step 82.

25 In step 82, the process applies a default email policy.
The default email policy tests for specific keywords in
messages, and for specific filetypes as attachments, in the
same way as the sender-specific email policies described
above. However, it is typically more restrictive in all
30 respects than the sender-specific email policies applied to
messages with verified digital signatures. That is, the
default email policy may have a longer list of keywords
which mark a message as non-compliant, or may regard more
different filetypes as non-compliant.
35

If it is determined in step 82 that the message complies with the default email policy, the process passes to step 78, and the message is allowed to be transmitted over the internet 25, as described above. If it is determined in

5   step 82 that the message does not comply with the default email policy, the process passes to step 80, and appropriate measures are applied, again as described above.

As mentioned above, the default email policy is typically

10 more restrictive in all respects than the sender-specific email policies applied to messages with verified digital signatures. Indeed, the default email policy may be such that no messages can comply with it. That is, all messages are rejected, unless they contain a verified digital

15 signature.

It is also possible to define a variable default email policy. For example, a message without a digital signature may result from a simple omission. On the other hand, a

20 message with a digital signature which does not match the purported sender identified in the message itself may be the result of a deliberate attempt to circumvent security procedures. Messages in these two categories may therefore be treated differently.

25

It is also possible to define a user-specific default email policy. For example, in the event that a message from one user or one of a group of users fails to include a verified digital signature, that message could be handled

30 differently from a situation in which a message from another user or one of another group of users fails to include a verified digital signature.

The invention has been specifically described above with

35 reference to its application in a boundary agent, to determine whether an email message can be transmitted

across a boundary, for example to determine whether an email message can be transmitted outside a corporate local area network. However, it will be appreciated that the same method can be applied at any point in a network, for

5   example within a local area network, to determine whether an email message can be further transmitted.

There is therefore disclosed a method of applying a sender-specific email policy based on a digital signature attached

10 to an email message, to determine whether it should be transmitted further over a network.